VASILE MAIEREAN – Spionaj. Falimentul unui sistem clandestin de comunicare impecabil?

(Din revista LUMEA nr.5 /2012)







Spionaj.
Falimentul unui sistem clandestin de comunicare impecabil?
- Legături unilaterale radio (LUR) -

Serviciul cubanez de informații externe (DGI) are o lungă tradiție a transmiterii mesajelor, către agentura din străinătate, prin stațiile radio pe unde scurte. Deși este o modalitate sigură de comunicare secretă, au fost cazuri când asemenea legături au fost descoperite, iar materialele găsite asupra spionilor au constituit probe directe pentru acuzare și condamnare.



Faptul că Statele Unite ale Americii constituie obiectivul principal al activității serviciului de informații externe al Republicii Cuba (Direccion General de Inteligentia - DGI), este în firea lucrurilor. De asemenea, realitatea că Federal Bureau of Investigation (FBI) și alte agenții guvernamentale americane specializate în contraspionaj, acționează pentru a descoperi cadrele DGI, nu este ceva insolit. Provocarea survine când obiectul de studiu este modul în care spionii cubanezi, descoperiți în ultimii ani în Statele Unite, și-au gestionat mesajele criptate primite de la Centrala din Havana prin clasicul sistem de recepție a emisiunilor radio unilaterale (LUR) pe unde scurte.

Ana Belen Montes a fost arestată și acuzată de spionaj, în anul 2001, în timp ce lucra ca analist principal la Defense Intelligence Agency (DIA) – Agenția de Informații a Armatei Statelor Unite. Procurorii au stabilit că aceasta primea instrucțiuni din partea DGI cubaneze prin intermediul mesajelor criptate recepționate din emisiuni radio pe unde scurte.

În 2006, **Carlos M. Alvarez Sanchez,** profesor asociat de învățământ și studii politice la Florida International University și soția acestuia **Elsa Prieto Alvarez,** au fost acuzați de spionaj în favoarea Cubei, fiind dovediți și că recepționau mesaje cifrate, transmise prin emisiuni radio pe unde scurte de către serviciul de informații cubanez.

Un funcționar al Departamentului de Stat, **Walter Kendall Myers** și soția sa, **Gwendolyn Steingraber,** au fost arestați și acuzați, în 2009, că acționau de aproape 30 de ani ca agenți ai DGI cubaneze. Și aceștia aveau în dotare un receptor radio prin care recepționau mesajele criptate transmise de DGI.

Pare neverosimil că un sistem criptografic considerat impecabil a furnizat totuși dovezi în cele trei cazuri. Erorile comise de spionii cubanezi în activitatea clandestină au condus, mai devreme sau mai târziu, la depistarea acestora, iar abaterile comise în procesul de exploatare a sistemului criptografic au oferit justiției americane posibilitatea să dispună și de **probe materiale directe** pentru acuzare și condamnare.

Oricine ascultă posturi radio pe unde scurte, poate întâlni emisiuni care transmit, vocal sau în sistemul Morse, grupe de cifre, pe care un spion le recepționează și le descifrează, primind astfel instrucțiuni pentru activitatea sa.

Avantajul unor asemenea transmisiuni este evident, emisiunile radio pe unde scurte realizează difuzarea, în timp real, în condiții de siguranță maximă, texte cifrate către agenți aflați în misiuni. Recepția se face cu orice aparat de radio care operează și în unde scurte. Deoarece este imposibil de a fi depistată persoana căruia îi este adresat mesajul, emisiunile LUR constituie o modalitate ideală de a se comunica cu **fantomele** (spioni plantați pe teritoriul străin cu identitate falsă), și cu **agenții deplin acoperiți** (care nu dispun de protecția oferită de imunitățile statutului diplomatic). Excepție face cazul în care agentul este deja sub monitorizarea contraspionajului și prin mijloace tehnice speciale este localizat în momentul în care recepționează mesajul, putând fi astfel prins în flagrant delict.

LUR au fost folosite pe scară largă în al Doilea Război Mondial, serviciile de informații britanice, americane, sovietice ș.a. comunicând astfel cu agenturile sau echipele lor de sabotaj din spatele liniilor inamicului. Pe timpul Războiului Rece, LUR au fost întrebuințate la fel de intens de către centralele de spionaj, pentru a transmite instrucțiuni agenților din țările despărțite de Cortina de Fier.

Precizăm, fără nici o intenție de malițiozitate, ca o constatare obiectivă a realităților de pe frontul **Războiului Mondial Permanent** al serviciilor secrete de informaţii, că sistemul se folosește cu aceeași dorită finalitate și în păstrarea legăturilor clandestine cu spionii care acționează, reciproc, chiar și în țări având parteneriate politice consacrate.

Înainte de a fi difuzate, mesajele sunt cifrate prin aplicarea de algoritmi criptografici. De obicei este folosit cifrul **OTP (one-time pad),** care s-a dovedit a fi, până acum, unicul criptosistem considerat perfect din punct de vedere teoretic, și practic impenetrabil, dacă este folosit în mod corect. In cadrul acestui sistem textul clar al mesajului este criptat cu un cifru de substituţie, supracifrat

cu o cheie aleatoare **(pad)** la fel de lungă ca şi lungimea mesajului, rezultând un text cifrat aleator. În cazul în care algoritmul este cu certitudine aleator, are lungimea mesajului, nu este refolosit niciodată parţial sau în întregime şi se asigură păstrarea lui într-un secret absolut, cifrul este imposibil de decriptat.

Criptarea se face prin convertirea textului clar al mesajului în grupe de cifre cu ajutorul unui careu de substituție, după care se supracifrează cu ajutorul algoritmului OTP, iar mesajul cifrat rezultat este transmis prin radio după un program și pe frecvențe convenite.

Sistemul de cifrare OTP este simplu și ușor de folosit, emitentul și cel care recepționează dispunând de chei identice, perfect aleatoare. Aceste chei, tipărite pe hârtie, legate în carnete sau transpuse pe microfilm, ușor de ascuns și de distrus în caz de necesitate, trebuie folosite numai o singură dată și distruse imediat după utilizare.

Example One-Time Pad

48173 19839 90183
51834 00182 47865
01983 47362 3 2
60120 98754 2 874

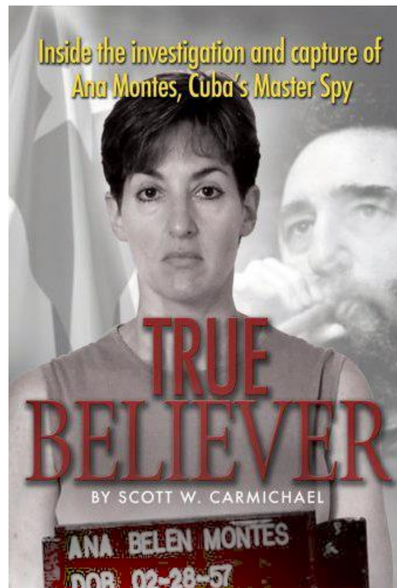
http://www.decodesystems.com/mt/98oct/crypt.html

SERIAL: 21813

77749 31977 32052 92381 25221
19041 79162 54244 23712 61891
41164 11238 11045 14519 25021
11323 31025 37019 95845 12017

DESTROY IMMEDIATELY AFTER USE

http://stuff.baturin.org/post/12680846183



http://www.latinamericanstudies.org/cuban-espionage.htm

Ana Belen Montes, născută în 1957, a obținut o diplomă în domeniul politicilor externe la University of Virginia și a terminat un masterat în studii politice internaționale avansate la Johns Hopkins University. A început să lucreze în Ministerul Justiției, din septembrie 1985, iar ulterior a trecut la DIA, promovând în funcția de analist principal pe probleme cubaneze și obținând accesul la date clasificate.

Opiniile sale cu privire la politica SUA față de țările Americii Latine au atras atenția serviciului de informații din Cuba, care a recrutat-o.

În 1996, un coleg din Agenție a raportat ofițerului de contrainformații că o suspectează pe Ana Belen Montes de a avea legături cu spionajul cubanez. Dosarul a fost însă clasat, fără a se face investigații amănunțite. Patru ani mai târziu, în timpul anchetării de către FBI a unui agent cubanez, au apărut din nou informații referitoare la ea.

În același an, Ana Belen Montes a fost instruită de serviciul de informații cubanez să achiziționeze un laptop și i s-au dat dischete de calculator pe care să le folosească la descifrarea mesajelor radio recepționate. De asemenea, a obținut dischete pentru cifrarea informațiilor culese în vederea trimiterii în centrală. Concomitent, a primit și un program de ștergere a mesajelor cifrate sau

descifrate din laptop. Pentru întâlniri și schimburi de dischete, ea apela un număr de pager, folosind cartele pre-plătite și utilizând coduri anterior stabilite pentru transmiterea de mesaje.

În acest context favorabil, FBI-ul nu a întâmpinat dificultăți pentru găsirea de probe directe, care au permis susținerea punerii sub acuzare a Anei Belen Montes, în septembrie 2001, și condamnării ei la 25 de ani de închisoare, pentru spionaj în favoarea Cubei, în octombrie 2002. Cu puțin timp înaintea arestării, în timpul unei percheziții secrete la locuința acesteia, FBI-ul a găsit laptopul și a copiat hard diskul (HDD), pe care l-a analizat, descoperind textele șterse, inclusiv instrucțiunile asupra modului de gestionare a mesajelor cifrate.

S-a dovedit astfel că folosirea calculatorului pentru cifrarea/descifrarea de mesaje este total improprie, deoarece informațiile stocate în memoria fișierelor, se regăsesc pe HDD și după ștergerea lor, iar software-urile de recuperare de date, capabile să refacă întregul conţinut al hard diskului, chiar şi după formatare, au o misiune relativ facilă în a le reconstitui.

Este de neînțeles cum serviciul de informații cubanez a decis să utilizeze o versiune software, în loc de a folosi cel mai sigur sistem criptografic, cel manual. Procedeul de cifrare/descifrare manuală asigură securitatea deplină a sistemului deoarece toate materialele se distrug imediat după folosirea lor, de regulă prin ardere. Această modalitate este foarte simplă. Pentru un mesaj de cca. 150 grupe nu sunt necesare mai mult de 30-40 de minute pentru a fi prelucrat, iar un cod scurt poate înlocui propoziții sau fraze întregi. Singurul motiv logic pentru folosirea software-ului, ar fi comoditatea și viteza de realizare a operațiunilor, însă, după cum s-a văzut, în această situație se neglijează un element esențial al funcționării sistemului, cel al asigurării unei securități depline a materialelor criptografice folosite.

Dacă Montes ar fi fost instruită să cifreze/descifreze mesajele manual, dovezile fizice de inculpare a sa ar fi fost mult mai greu, sau chiar imposibil, de găsit.



Carlos M. Alvarez Sanchez şi Elsa Prieto Alvarez
http://www.latinamericanstudies.org/alvarez-espionage.htm

Carlos M. Alvarez Sanchez (n. 1944) și soția sa, **Elsa Prieto Alvarez** (n.1950) s-au născut în Cuba. Carlos Alvarez a devenit cetățean american în 1972, iar soția sa în 1979. Carlos Alvarez, doctor în psihologie clinică, era profesor-asociat, șeful catedrei de învățământ și studii politice la Florida International University (UIF). Elsa era asistent social și consilier psihologic la aceeași universitate.

Carlos Alvarez a început să transmită informații spionajului din Cuba în 1977. În 1982, după căsătoria lor, Elsa a început să lucreze, o perioadă în mod independent, pentru DGI cubaneză, ulterior făcând echipă cu soțul ei, cei doi având, ca nume de cod, pseudonimul **Deborah** și, respectiv, **David**. Cuplul de spioni a acționat, timp de peste trei decenii, pentru a culege și transmite informații cu privire la comunitatea exilului cubanez și referitoare la evenimente de interes pentru regimul castrist.

Cel care fusese instruit pentru a cifra și descifra mesajele de la/către serviciul de informații cubanez, comunicând cu acesta printr-o varietate de moduri, era Carlos Alvarez. El primea instrucțiunile pe calea transmiterilor radio pe unde scurte. Odată recepționate, mesajele erau descifrate cu ajutorul unei dischete care conținea software-ul de decriptare. În mod similar, se folosea o altă dischetă pentru cifrarea mesajelor pe calculator. Dischetele cu mesajele cifrate erau depuse în diverse căsuțe poștale impersonale (CPI) din teritoriu, fiind preluate de alți agenți ai spionajului cubanez care le transportau în Cuba. După

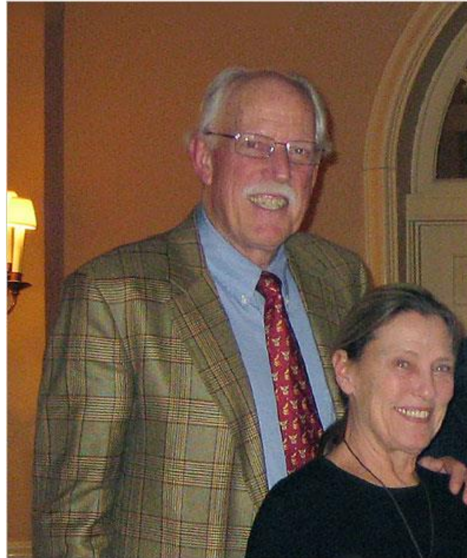
fiecare operațiune de cifrare-descifrare, Carlos era convins că distrugea toate dovezile electronice și digitale din calculator, ștergând, printr-o banală manevră de **delete**, materialele folosite.



Fiul cuplului Alvarez (dreapta),
care nu a cunoscut activităţile clandestine ale părinţilor săi,
după condamnarea celor doi spioni,
a declarat laconic: “Sunt extreme de supărat!”.
http://www.latinamericanstudies.org/alvarez-espionage.htm

În 2005, după ce au primit unele informații despre activitățile suspecte ale soților Alvarez, autoritățile americane (FBI-ul și Naval Criminal Investigative Service – **NCIS** – Serviciul de Investigație Penală al Marinei) au început să îi monitorizeze, efectuând și precheziții secrete la locuința acestora. Analizând unitatea HDD a calculatorului, specialiștii informaticieni ai FBI au descoperit mesaje codificate, ceea ce a dus la imediata lor arestare.

După cum se poate observa, între cele două cazuri prezentate există o serie de similitudini. În ambele situații, după ce s-au primit informații despre acțiunile lor suspecte, au fost supravegheați și li s-au percheziționat în secret locuințele, descoperindu-se dovezi cu privire la activitățile de spionaj. Cu toate că Alvarez a fost mai precaut, acționând consecvent, conform instructajului, pentru distrugerea materialelor folosite la cifrarea/descifrarea mesajelor, datele, odată procesate prin calculator, nu au fost înlăturate din măruntaiele teribilei mașinării electronice. Din nou, un sistem criptologic sigur a fost compromis de decizia greșită de folosire a calculatorului pentru realizarea operațiunilor de cifrare/descifrare a mesajelor.



Walter Kendall Myers şi Gwendolyn Steingraber Myers
http://www.latinamericanstudies.org/cuban-espionage.htm

Walter Kendall Myers (n. 1937), este **strănepotul** lui Alexander Graham Bell, inventator al telefonului și este **nepotul** lui Gilbert Hovey Grosvenor, **„**tatăl fotojurnalului" și redactor șef al revistei National Geografic, timp de 55 de ani. G. H. Grosvenor a fost **văr** cu William Howard Taft, al 27-lea președinte al SUA (1909 – 1913).

Walter Kendall Myers a servit în cadrul United States Army Security Agency (ASA) - Agenția de Securitate a Armatei, din 1959 până în 1962, primind o instruire intensivă în comunicații. A urmat apoi Brown University și a obținut doctoratul la Johns Hopkins University, unde a și activat, timp de 20 de ani, ca profesor de studii europene. Din 1977, a fost încadrat la Departamentul de Stat, lucrând inițial la Foreign Service Institute (FSI) – Institutul Serviciului Extern - ca instructor, apoi ca analist la Bureau of Intelligence and Research (INR) - Biroul de Informații și Cercetare, dispunând de un certificat de securitate pentru accesul la informații clasificate de înalt nivel, până în 2007, când s-a pensionat.

În 1978, Myers și soția sa, **Gwendolyn Steingraber Myers,** călătoriseră în Cuba în interes personal și academic, invitați de guvernul cubanez prin misiunea sa diplomatică din Statele Unite. Cu acest prilej, soții Myers și-au

exprimat o afinitatea puternică față de politica acestei țări și profunde sentimente negative la adresa sistemului capitalist american. Apreciind comportamentul și atitudinea lor, DGI cubaneză i-a recrutat ca spioni, instruindu-i cum să acționeze și stabilindu-le numele de cod **202** și **E-634**.

W. K. Myers a realizat sistematic întâlniri cu ofițeri de legătură ai DGI cubaneză în țări precum Trinidad-Tobago, Jamaica, Brazilia, Ecuador, Argentina, Mexic. Cunoscând semnalele Morse, Myers primea instrucțiuni prin mesaje radio transmise pe unde scurte, dispunând de un receptor asemănător cu cel al Anei Belen Montes.

Myers sustrăgea informații clasificate de la locul său de muncă din Departamentul de Stat, pe care le transmitea ofițerului de contact în cadrul unor întâlniri fulger de predare-primire **(mână la mână)**. După arestarea Anei Belen Montes, ca o măsură de precauție, Myers a început să furnizeze informațiile în cadrul unor contacte realizate în afara teritoriului american.

În cadrul supravegherilor informative generale, FBI-ul a făcut o analiză a frecventelor deplasări în străinătate ale soților Myers, finalizată cu suspiciunea că aceștia ar putea lucra pentru un serviciu de spionaj străin, fapt ceea ce a determinat declanșarea măsurilor specifice de monitorizare a cuplului.

În 2009, când deja Myers se pensionase, FBI-ul a început o operațiune clandestină: un agent sub acoperire s-a prezentat la acesta susținând că a fost trimis de un ofițer cubanez de legătură pentru a-l contacta și a-i cere să obțină unele informații. În timpul unor întâlniri ulterioare, fiind convins că vorbește cu un autentic ofițer de informații cubanez, Myers a făcut dezvăluiri despre activitatea sa de spionaj timp de peste 30 de ani în favoarea Cubei, prezentând și detaliile diverselor operațiuni. Printre acestea, s-a referit și la modalitatea de primire a instrucțiunilor transmise prin emisiuni radio pe unde scurte. O analiză a computerului de la serviciu al lui Myers, făcută de FBI, a arătat că, numai în ultimul an de serviciu, el cercetase mai mult de 200 de rapoarte clasificate privind Cuba.

Walter Kendall Myers și Gwendolyn Steingraber Myers au fost arestați în iunie 2009, ca punct culminant al unei acțiuni desfășurate timp de trei ani, a FBI-ului și a State Departament's Bureau of Diplomatic Security (DS) - Biroul de Securitate Diplomatică din Departamentul de Stat al SUA, finalizată prin **condamnarea la închisoare pe viață a lui W. K. Myers si la 6 ani de închisoare a soției sale.**

Cazul Meyers este un elocvent exemplu privind modul în care poate fi descoperit un spion printr-o acțiune sub acoperire, informațiile obținute și confirmate, apoi, în cursul anchetei procuraturii, incriminându-l indubitabil pe acesta. Transmiterea mesajelor pe calea undelor scurte ale stațiilor radio s-a folosit și în acest caz. Cu toate că FBI-ul nu a reușit să descopere probe cu mesaje cifrate/descifrate, în instanță s-au prezentat declarațiile de recunoaștere a folosirii LUR, precum și dovezi cu înregistrări ale mesajelor primite pe această cale, rezultate din interceptările efectuate în timpul supravegherii sale.

Concluzionând, rămânem stupefiați să constatăm că un sistem de criptare sigur, cu hârtia și creionul, a putut fi înlocuit, chiar într-un cadru instituțional ultra-specializat - un serviciu de informații național -, printr-o aplicație informatică nesigură. Descifrarea manuală a unui volum rezonabil de mesaje recepționate prin radio și distrugerea tuturor materialelor folosite pentru această operațiune, ar fi asigurat securitatea deplină a comunicațiilor. Serviciul de informații cubanez nu a luat în considerare, dintr-o rușinoasă ignoranță profesională, sau dintr-o negljență criminală, faptul că, în momentul trecerii de la sistemul de criptare manual, la cel prelucrat prin software, ar fi trebuit să țină seama de noile și dificilele probleme de securitate pe care le presupune metoda de cifrare/descifrare cu ajutorul calculatorului.

Dezvoltate în arii de obținere a informațiilor diferite, cazurile expuse mai sus, au avut totuși în comun două elemente definitorii:

1. Baza motivațională, constituită din convingeri ideologice, și nu din interes pecuniar, care a determinant o continuă influență benefică pentru intensitatea și calitatea acțiunilor specfice de spionaj, desfășurate perioade foarte lungi de timp;
2. Generalizarea, în ultima perioadă a misiunilor clandestine, de către serviciul de informații cubanez, cu efecte catastrofale în final, a utilizării practicii sinucigașe de folosire a sistemelor informatice moderne în gestionarea materialelor criptografice de către agenții operaționali.

S-a înregistrat, deci, falimentul unui sistem de legătură considerat impecabil?

Spețele dezvoltate de noi arată că modalitatea de a transmite,
prin emisiuni radio pe unde scurte de tip LUR,
mesaje criptate cu cifrul ONE-TIME PAD,
este sigură.

Nici unul dintre agenți nu a fost descoperit datorită decriptării acestor mesaje, ei ajungând să fie arestați în urma unor informații obținute prin complexe investigații contrainformative.

A fost practicat un sistem criptologic perfect (teoretic și practic),
fără a se ține însă cont de vulnerabilitățile
pe care le implică folosirea computerului.
Pe cale de consecință, pe frontul dur al serviciilor secrete de informații,
o asemenea greșeală inacceptabilă se plătește scump,
inevitabil prin depistarea și condamnarea s(pionilor),
uneori la închisoare pe viaţă sau chiar la moarte.

Gen.br. (r) **Vasile MAIEREAN**





http://www.worldatlas.com/webimage/countrys/namerica/caribb/lgcolor/cucolor.htm